



AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 1-24 (Canceled).

1 25. (Currently amended) A method for managing encryption within a
2 database system, wherein encryption is performed automatically and transparently
3 to a user of the database system, the method comprising:

4 receiving a request at the database system to store data in the database
5 system;

6 wherein the request is directed to one or more columns of the database
7 system that have been designated as encrypted;

8 in response to the request:

9 | creating a digest of the data using a cryptographic function,

10 | and

11 | automatically encrypting the data within the database

12 system using an encryption function and an encryption key ,

13 wherein information about the encryption key is stored in a

14 metadata table, which includes information identifying the

15 cryptographic function used to create the digest; and

16 storing the encrypted data in the database system.

17

1 26. (Previously presented) The method of claim 25,

2 wherein the encryption function uses a key stored in a keyfile managed by
3 a security administrator; and
4 wherein the encrypted data is stored using a storage function of the
5 database system.

1 27. (Currently amended) The method of claim 26, further comprising:
2 receiving a request to retrieve data from a column ~~the column~~ of the
3 database system;
4 if the request to retrieve data is received from a database administrator,
5 preventing the database administrator from decrypting the encrypted data;
6 if the request to retrieve data is received from the security administrator,
7 preventing the security administrator from decrypting the encrypted data; and
8 if the request to retrieve data is from an authorized user of the database
9 system, allowing the authorized user to decrypt the encrypted data.

1 28. (Currently amended) The method of claim 26, wherein the security
2 administrator selects one of, data encryption standard (DES) and triple DES as a
3 mode of encryption for a column ~~the column~~.

1 29. (Previously presented) The method of claim 26, wherein the security
2 administrator, a database administrator, and a user administrator are distinct roles,
3 and wherein a person selected for one of these roles is not allowed to be selected
4 for another of these roles.

1 30. (Currently amended) The method of claim 26, wherein managing the
2 keyfile includes, but is not limited to:
3 creating the keyfile;
4 establishing a plurality of keys to be stored in the keyfile;

5 establishing a relationship between a key identifier and the key stored in
6 the keyfile;
7 storing the keyfile in one of,
8 an encrypted file in the database system, and
9 a location separate from the database system; and
10 | moving the obfuscated copy of the keyfile to a volatile~~the volatile~~
11 memory within a server associated with the database system.

1 31. (Currently amended) The method of claim 30, wherein the key
2 | identifier associated with a column~~the column~~ is stored as metadata associated
3 with a table containing the column within the database system.

1 32. (Currently amended) The method of claim 30, further comprising
2 | establishing encryption parameters for a column~~the column~~, wherein encryption
3 parameters include encryption mode, key length, and integrity type by:
4 entering encryption parameters for the column manually; and
5 recovering encryption parameters for the column from a profile table in the
6 database system.

1 33. (Currently amended) The method of claim 26, wherein upon receiving
2 | a request from the security administrator specifying a column~~the column~~ to be
3 encrypted, if the column currently contains data, the method further comprises:
4 decrypting the column using an old key if the column was previously
5 encrypted; and
6 encrypting the column using a new key.

1 34. (Currently amended) A computer-readable storage medium storing
2 instructions that when executed by a computer causes the computer to perform a

3 method for managing encryption within a database system, wherein encryption is
4 performed automatically and transparently to a user of the database system, the
5 method comprising:

6 receiving a request at the database system to store data in the database
7 system;

8 wherein the request is directed to one or more columns of the database
9 system that have been designated as encrypted;

10 in response to the request:

11 | creating a digest of the data using a cryptographic function,

12 and

13 | automatically encrypting the data within the database

14 system using an encryption function and an encryption key ,

15 wherein information about the encryption key is stored in a

16 metadata table, which includes information identifying the

17 cryptographic function used to create the digest; and

18 storing the encrypted data in the database system.

1 35. (Previously presented) The computer-readable storage medium of
2 claim 34,

3 wherein the encryption function uses a key stored in a keyfile managed by
4 a security administrator; and

5 wherein the encrypted data is stored using a storage function of the
6 database system.

1 36. (Currently amended) The computer-readable storage medium of claim
2 35, the method further comprising:

3 | receiving a request to retrieve data from a column ~~the column~~ of the
4 database system;

5 if the request to retrieve data is received from a database administrator,
6 preventing the database administrator from decrypting the encrypted data;
7 if the request to retrieve data is received from the security administrator,
8 preventing the security administrator from decrypting the encrypted data; and
9 if the request to retrieve data is from an authorized user of the database
10 system, allowing the authorized user to decrypt the encrypted data.

1 37. (Currently amended) The computer-readable storage medium of claim
2 35, wherein the security administrator selects one of, data encryption standard
3 (DES) and triple DES as a mode of encryption for a column ~~the column~~.

1 38. (Previously presented) The computer-readable storage medium of
2 claim 35, wherein the security administrator, a database administrator, and a user
3 administrator are distinct roles, and wherein a person selected for one of these
4 roles is not allowed to be selected for another of these roles.

1 39. (Currently amended) The computer-readable storage medium of claim
2 35, wherein managing the keyfile includes, but is not limited to:
3 creating the keyfile;
4 establishing a plurality of keys to be stored in the keyfile;
5 establishing a relationship between a key identifier and the key stored in
6 the keyfile;
7 storing the keyfile in one of,
8 an encrypted file in the database system, and
9 a location separate from the database system; and
10 | moving the obfuscated copy of the keyfile to a volatile ~~the volatile~~
11 memory within a server associated with the database system.

1 40. (Currently amended) The computer-readable storage medium of claim
2 39, wherein the key identifier associated with the column is stored as metadata
3 associated with a table containing a column~~the column~~ within the database
4 system.

1 41. (Currently amended) The computer-readable storage medium of claim
2 39, wherein the method further comprises establishing encryption parameters for a
3 column~~the column~~, wherein encryption parameters include encryption mode, key
4 length, and integrity type by:
5 entering encryption parameters for the column manually; and
6 recovering encryption parameters for the column from a profile table in the
7 database system.

1 42. (Currently amended) The computer-readable storage medium of claim
2 35, wherein upon receiving a request from the security administrator specifying a
3 column~~the column~~ to be encrypted, if the column currently contains data, the
4 method further comprises:
5 decrypting the column using an old key if the column was previously
6 encrypted; and
7 encrypting the column using a new key.

1 43. (Currently amended) An apparatus that facilitates managing encryption
2 within a database system, wherein encryption is performed automatically and
3 transparently to a user of the database system, comprising:
4 a receiving mechanism that is configured to receive a request at the
5 database system to store data in the database system;
6 wherein the request is directed to one or more columns of the database
7 system that have been designated as encrypted;

8 a digest creating mechanism configured to create a digest of the data using
9 a cryptographic function;
10 an encrypting mechanism that is configured to automatically encrypt the
11 data within the database system using an encryption function and an encryption
12 key , wherein information about the encryption key is stored in a metadata table,
13 which includes information identifying the cryptographic function used to create
14 the digest; and
15 a storing mechanism that is configured to store the encrypted data in the
16 database system.

1 44. (Previously presented) The apparatus of claim 43,
2 wherein the encryption function uses a key stored in a keyfile managed by
3 a security administrator; and
4 wherein the encrypted data is stored using a storage function of the
5 database system.

1 45. (Currently amended) The apparatus of claim 44, further comprising:
2 the receiving mechanism that is further configured to receive a request to
3 retrieve data from a column ~~the column~~ of the database system;
4 an access mechanism that is configured to prevent a database administrator
5 and the security administrator from decrypting the encrypted data; and
6 wherein the access mechanism is configured to allow an authorized user
7 of the database system to decrypt the encrypted data.

1 46. (Currently amended) The apparatus of claim 44, further comprising a
2 selection mechanism that is configured to select one of, data encryption standard
3 (DES) and triple DES as a mode of encryption for a column ~~the column~~.

1 47. (Previously presented) The apparatus of claim 44, wherein the security
2 administrator, a database administrator, and a user administrator are distinct roles,
3 and wherein a person selected for one of these roles is not allowed to be selected
4 for another of these roles.

1 48. (Currently amended) The apparatus of claim 44, further comprising:
2 a creating mechanism that is configured to create the keyfile;
3 an establishing mechanism that is configured to establish a plurality of
4 keys to be stored in the keyfile;
5 wherein the establishing mechanism is further configured to establish a
6 relationship between a key identifier and the key stored in the keyfile;
7 wherein the storing mechanism is further configured to store the keyfile in
8 one of,
9 an encrypted file in the database system, and
10 a location separate from the database system; and
11 a moving mechanism that is configured to move the obfuscated copy of
12 the keyfile to a volatile ~~the volatile~~ memory within a server associated with the
13 database system.

1 49. (Currently amended) The apparatus of claim 48, wherein the key
2 identifier associated with a column ~~the column~~ is stored as metadata associated
3 with a table containing the column within the database system.

1 50. (Currently amended) apparatus of claim 48, wherein the establishing
2 mechanism is further configured to establish encryption parameters for a column
3 ~~the column~~, wherein encryption parameters include encryption mode, key length,
4 and integrity type, and wherein the establishing mechanism includes:

5 an entering mechanism that is configured to enter encryption parameters
6 for the column manually; and
7 a recovering mechanism that is configured to recover encryption
8 parameters for the column from a profile table in the database system.

1 51. (Currently amended) The apparatus of claim 44, further comprising:
2 | a decrypting mechanism that is configured to decrypt a column~~the column~~
3 using a previous key if the column was previously encrypted; and
4 wherein the encrypting mechanism is further configured to encrypt the
5 column using a new key.